TACTICAL MANET ATTACK DETECTION BASED ON FUZZY SETS USING AGENT COMMUNICATION

Damian Watkins

Knowledge Management Center of Excellence (KMCOE)
Morgan State University
School of Engineering
5200 Perring Parkway
Baltimore, MD 21251

ABSTRACT[†]

This study describes a distributed attack detection approach for a tactical MANET using intelligent agents equipped with inference systems based on fuzzy logic. The results produce a prototype intrusion detection system capable of effectively detecting attacks in a tactical MANET with accuracy approaching 95%. The attack recognition system is implemented using stationary intelligent fuzzy agents (SIFA) resident on each node. Agents run autonomously on each node, collect packets from the data stream, extract relevant information, exchange information through light-weight messages, and trigger alerts using the fuzzy inference process.

1. INTRODUCTION

The work presented in this paper is supported by the Army Research Laboratory (ARL) Collaborative Technology Alliance (CTA). Technical Area 4 encompasses tactical information protection involving attack recognition and event dissemination where attack recognition is the focus of this study. The objective of the attack recognition effort is to develop inference and correlation technologies that can detect complex multi-stage attacks in MANET environments where the reliance on centralized mechanisms or fixed relationships is unattainable. Attack detection in a tactical mobile ad-hoc network (MANET) environment is a daunting task due to its wide open and dynamic characteristics [Zhang et al., 2003]. In the battlefield arena, use of peer-to-peer wireless ad-hoc networks by the army may bestow a multitude of vulnerabilities within the network that may prove detrimental to the users of that system. Preliminary studies have shown that traditional approaches to intrusion detection may be inadequate for effective detection in an environment with dropping nodes and rapidly changing network topologies stemming from node movements [Watkins, 2004]. In a MANET environment one can surmise that conventional intrusion detection systems may have difficulty performing as designed for three reasons [Zhang et al. 2003, Athanasades et al., 2003]:

1. The limited bandwidth of the environment may limit the amount of data necessary for adequate detection.
2. The dynamic nature of the environment such as changing topologies may blind the IDS from full view of the network.
3. Overhead associated with the IDS that enable packet sniffing and processing may significantly reduce network performance.

The result of this effort produced a prototype intrusion detection system capable of effectively detecting attacks in a tactical MANET with accuracy approaching 95%. The attack recognition system is implemented using stationary intelligent fuzzy agents (SIFA) resident on each node. SIFA is essentially a rule-based processing system for attack recognition in a MANET environment. The reasoning system has three parts: A knowledge-base (set of if-then rules); a working memory or database of derived facts; and an inference engine containing the reasoning logic used to process the knowledge base. Agents run autonomously on each node, collect packets from the data stream, extract relevant information, exchange information through light-weight messages, and trigger alerts using the fuzzy inference process.

2. RESEARCH METHODOLOGY

The research methodology was conducted in two phases. First, a representative tactical MANET was characterized and analyzed for which a representative data set was produced. Secondly, the SIFA application was developed and tested on the dataset. The results suggest a plausible technique for performing intrusion detection in a dynamic tactical MANET. The relative success or failure of the attacker as well as the effectiveness of a conventional intrusion detection system was analyzed in various topologies. Each topology from a routing perspective in the MANET environment presents advantages for an attacker to successfully footprint, scan, enumerate, and hack without detection. Certain topologies also present advantages for the IDS where attacks are more difficult to execute but are easier to detect [Watkins, 2004].

[†] Prepared through collaborative participation in the Collaborative Technology Alliance for Communications and Networks sponsored by the U.S. Army Research Laboratory under Cooperative Agreement DAAD19-01-2-0011. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 DEC 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Tactical Manet Attack Detection Based On Fuzzy Sets Using Agent Communication	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Knowledge Management Center of Excellence (KMCOE) Morgan State University School of Engineering 5200 Perring Parkway Baltimore, MD 21251**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida. , The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**2**	

3. APPLICATION DESCRIPTION

A fuzzy set is a collection of objects with membership values between 0 (complete exclusion) and 1 (complete membership) [Zadeh, 1998, Nguyen, 2000]. Membership functions associated with fuzzy sets are dependent on the concept being represented and the context for which it is used. The context of the application determines if the shape of the membership function is suitable. Each agent contains its own knowledge base and is responsible for a three-step procedure. The first step is to collect information from the data stream. Packets must be collected and information contained in packet headers must be extracted for used by the inference system. The second step involves the interpretation of the data for use in the fuzzy inference system. In the final step, the interpreted data is analyzed by the system to produce a result based on rules defined in the rule base and information from cooperating agents in the network. The ability of the agent to successfully detect malicious activity is highly dependent on the design of an adequate fuzzy model. The advantage of this research is the availability of data from a representative tactical MANET environment that is used to examine the viability of this approach.

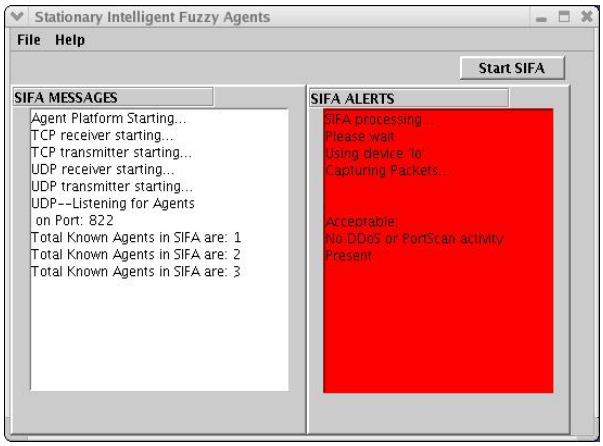

Figure1: SIFA Application

4. APPLICATION TESTING

The SIFA application was tested on the dataset for its ability to check for port scanning and distributed denial of service attacks. The TCPreplay open source program was used to retransmit packets over the network [Turner 2004]. Testing was conducted in this manner in order to demonstrate SIFA agent packet collection in real-time. The node network view is controlled using a topology manager where the node will see only the traffic that is delegated by the topology. In the test scenario, laptops were used to impersonate MANET nodes. The SIFA application was installed on all nodes. The traffic dump files were replayed over the local loop back interface and the laptops were connected wirelessly using 802.11b in Ad Hoc mode. The wireless medium was used to pass messages between agents and to broadcast live agents for the contact list. In different attack scenarios the SIFA application on each host should all agree on the number of live agents on the system and come to the same decision to trigger an alert.

5. CONCLUSION

Agents in the SIFA application were successfully able to cooperate and send messages using TCP and UDP protocols. The application was benchmarked in an off-line testing environment using TCP replay program. The application was able to successfully identify distributed denial of service attacks and port scanning attacks within the representative data set. It was also showed the ability to discern between multiple attack types. The work presented in this paper aims to provide a starting point for work in an immature research area. The goal of this research is to present basic methodologies for collecting, analyzing, and processing data for future development of MANET base intrusion detection systems.

Conclusion.[‡]

REFERENCES

Athanasades, Nicholas, Abler, Randal, Levine, John, Owen, Henry, and Riley, George, "Intrusion Detection Testing and Benchmarking Methodologies", Proceedings of the First IEEE International Workshop on Information Assurance, 2003, 1-10.

D. Watkins, C. Scott, "Methodology for Evaluating the Effectiveness of Intrusion Detection in Tactical Mobile Ad-hoc Networks", IEEE Wireless Communications and Networking Conference 2004, 1 -5.

Nguyen, Hung T., Walker, Elbert A., *A First Course in Fuzzy Logic 2nd Ed*, Chapman and Hall, 2000, 4-18.

Turner, Aaron, Tcpreplay FAQ http://tcpreplay.sourceforge.net/FAQ.html (9/20/2004).

Zadeh, Lotfi, "Fuzzy Logic", IEEE-CS Computer Volume 21, Number 4, April1998, 1-11

Zhang, Yongguang, Lee, Wenke, and Huang, Yi-An, "Intrusion Detection Techniques for Mobile Wireless Networks, Mobile Networks and Applications 2003, 1-9.

[‡] The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government.